



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,120	12/17/2001	Tomoyuki Asano	SONY JP -139	6143
530	7590	10/17/2005	EXAMINER	
LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK 600 SOUTH AVENUE WEST WESTFIELD, NJ 07090			CHAI, LONGBIT	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/937,120

Applicant(s)

ASANO ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 11 July 2005.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-178 is/are pending in the application.  
4a) Of the above claim(s) 47-101 and 137-178 is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-46 and 102-136 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 19 February 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 7/11/2005.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### *Election / Restrictions*

1. Examiner acknowledges that Applicant has elected Group I, Claim 1 – 46 and 102 – 136 without traverse.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 130 recites the limitation "said contents check value generation key". There is insufficient antecedent basis for this limitation in the claim.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 130 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claim 130 "executing encryption processing applying said contents check value generation key to said contents intermediate

Art Unit: 2131

value" is not enabled by the specification. As understood by the examiner, based upon the specification on paragraph [0172] and paragraph [0044], the contents check value generation key is applied to the contents block data to be checked as a message instead of being applied to said contents intermediate value.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1 – 3, 7, 8, 12, 19 – 21, 24, 25, 29, 36 – 38, 41, 42, 46, 102, 108, 111, 115, 121, 124, 128, 133 and 136 are rejected under 35 U.S.C. 102(b) as being anticipated by Orrin (Patent Number: 6011849).

As per claim 1, 19, 36, 46, 102, 115, 128 and 136, Orrin teaches a data processing apparatus for processing content data provided by a recording or communication medium, characterized in that said apparatus comprises:

a cryptography process section for executing a cryptography process on said content data (Orrin: Figure 1 Element 1); and

a control section for executing control for said cryptography process section (Orrin: Figure 1 Element 4), and

said cryptography process section:

Art Unit: 2131

is configured to generate partial integrity check values as integrity check values for a partial data set containing one or more partial data obtained by a content data-constituting section into a plurality of parts, and to collate the generated integrity check values to verify said partial data (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67), and

generates an intermediate integrity check value based on a partial integrity check value set data string containing at least one or more of said partial integrity check values, and uses the generated intermediate integrity check value to verify the entirety of the plurality of partial data sets corresponding to the plurality of partial integrity check values constituting said partial integrity check value set (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

As per claim 2, 20, 37, 108, 121 and 133, Orrin teaches said partial integrity check value is generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using partial data to be checked, as a message, said intermediate integrity check value is generated by means of a cryptography process with an general-check-value-generating key applied thereto, using a partial integrity check value set data string to be checked, as a message, and said cryptography process section is configured to store said partial-integrity-check-value-generating value and said general-integrity-check-value-generating key (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

Art Unit: 2131

As per claim 3, 21 and 38, Orrin teaches said cryptography process has plural types of partial-check-value-generating key corresponding to generated partial integrity check values (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

As per claim 7, 24 and 41, Orrin teaches said data processing apparatus has a signature key, and said cryptography process section: is configured to apply a value generated from said intermediate value by means of said signature key-applied cryptography process as a collation value for data verification (Orrin: Column 7 Line 30 – 41).

As per claim 8, 25 and 42, Orrin teaches said data processing apparatus has a plurality of different signature keys as signature keys, and said cryptography process section: is configured to apply one of said plurality of different signature keys which is selected depending on a localization of said content data, to the cryptography process for said intermediate integrity check value to obtain the collation value for data verification (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67).

As per claim 12, 29, 111 and 124, Orrin teaches a recording device for storing data validated by said cryptography process section (Orrin: Column 8 Line 38 – 47).

Art Unit: 2131

As per claim 17, Orrin teaches a data processing apparatus for processing content data provided by a recording or communication medium, characterized in that said apparatus comprises:

a cryptography process section for executing a cryptography process on said content data; and a control section for executing control for said cryptography process section, and said cryptography process section: is configured to generate, if data to be verified are encrypted, integrity check values for the data to be verified by means of a signature data-applied cryptography process from data on arithmetic operation results obtained by executing an arithmetic operation process on decrypted data (Orrin: Column 7 Line 40 – 41: a decrypted text from an encrypted content is equivalent to a plain text) obtained by executing a decryption process on the encrypted data (Orrin: Column 7 Line 40 – 41, Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67)

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2131

5. Claims 4 – 6, 22, 23, 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Teppler (Patent Number: 6898709).

As per claim 4, 22 and 39, Orrin does not disclose expressly said cryptography process is a DES cryptography process, and said cryptography process section is configured to execute the DES cryptography process.

Teppler teaches said cryptography process is a DES cryptography process, and said cryptography process section is configured to execute the DES cryptography process (Teppler: Column 7 Line 12 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Teppler within the system of Orrin because Teppler teaches providing the assurance of the integrity of digital data files with enhanced fraud prevention mechanisms (Teppler: Column 16 Line 36 – 52).

As per claim 5, 23 and 40, Orrin does not disclose expressly said partial integrity check value is a message authentication code (MAC) generated in an DES-CBC mode using partial data to be checked, as a message, said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message, and said cryptography process section is configured to execute the cryptography process in the DES-CBS mode.



Art Unit: 2131

Teppler teaches said partial integrity check value is a message authentication code (MAC) generated in an DES-CBC mode using partial data to be checked, as a message, said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message, and said cryptography process section is configured to execute the cryptography process in the DES-CBS mode (Teppler: Column 30 Line 48 – 53).

Same rationale of combination applies here as above in rejecting claim 4.

As per claim 6, Orrin as modified teaches in the DES-CBC mode-based cryptography process configuration of said cryptography process section, Triple DES is applied only in part of a message string to be processed (Teppler: Column 30 Line 48 – 53 and (Teppler: Column 7 Line 12 – 24).

6. Claims 9, 26 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Kuroda (Patent Number: 6915434).

As per claim 9 and 26 and 43, Orrin does not disclose expressly said data processing apparatus has a common signature key common to all entities of a system for executing a data verifying process and an apparatus-specific signature key specific to each apparatus that executes a data verifying process.

Art Unit: 2131

Kuroda teaches said data processing apparatus has a common signature key common to all entities of a system for executing a data verifying process and an apparatus-specific signature key specific to each apparatus that executes a data verifying process (Kuroda: Abstract Line 1 – 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kuroda within the system of Orrin because Kuroda teaches providing a key management function in an electronic data storage system for guaranteeing the security of electronic data by changing the key used in a process of encrypting electronic data in document form in a local environment and a global environment (Kuroda: Column 1 Line 10 – 16).

7. Claims 10, 11, 27, 28, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Nessett (Patent Number: 6055236).

As per claim 10, 27 and 44, Orrin teaches a digital signature stored in the header section (Orrin: Column 8 Line 1 – 3). However, Orrin does not disclose expressly a header section integrity check values generated for intra-header-section data partly constituting data.

Nessett teaches a header section integrity check values generated for intra-header-section data partly constituting data (Nessett: Column 23 Line 40 – 45).

Art Unit: 2131

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nessett within the system of Orrin because (a) Orrin discloses a basic key transfer process utilized by the file and document security systems via electronic mail or a network system through a horizontal trust model (Orrin: Column 4 Line 21 – 3) and (b) Nessett teaches providing enhanced internet security services using authentication header (Nessett: Column 3 Line 44 – 50).

Accordingly, Orrin in view of Nessett teaches:

said partial integrity check value contains one or more header section integrity check values generated for intra-header-section data partly constituting data and one or more content integrity check values generated for content block data partly constituting the data, and said cryptography process is configured to generate one or more header section integrity check values for a partial data set in said intra-header-section data to execute a collation process, generate one or more content integrity check values for a partial data set in said intra-content-section data to execute a collation process, and further generate a general integrity check value based on all said header section integrity check values and said content integrity check values generated, to execute a collation process in order to verify the data (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67; Nessett: Column 23 Line 40 – 45).

As per claim 11, 28 and 45, the claim limitations are met as the same reasons as that set forth in rejecting claim 10.

Art Unit: 2131

8. Claims 13 – 15, 30 – 32, 112 – 114 and 125 – 127 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Bodo (Patent Number: 5680587).

As per claim 13, 30, 112, 125 and 127, Orrin does not disclose expressly said control section is configured so that if in the process executed by said cryptography process section to collate the partial integrity check value, the collation is not established, and said control section suspends the process for storing data in said recording device.

Bodo teaches said control section is configured so that if in the process executed by said cryptography process section to collate the partial integrity check value, the collation is not established, and said control section suspends the process for storing data in said recording device (Bodo: Column 13 Line 16 – 25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bodo within the system of Orrin because (a) Orrin discloses invoking secure digital data content backup to removable media such as floppy disks (Orrin: Figure 7 and Column 8 Line 38 – 47) and (b) Bodo teaches an enhanced-performance floppy diskette subsystem for securely recording the digital data (Bodo: Column 13 Line 16 – 25).

Art Unit: 2131

As per claim 14, 31, 113 and 126, claims 14, 31, 113 and 126 do not further teach over claims 13 as addressed above

As per claim 15, 32 and 114, claims 15, 32 and 114 do not further teach over claims 13 as addressed above.

9. Claims 17, 18, 34, 35 103 – 105, 109, 110, 116, 117, 118, 122, 123, 129, 130, 134 and 135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Scott (Patent Number: 5199073).

As per claim 109, 122 and 134, Orrin does not teach said encryption processing section generates a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the content.

Scott teaches said encryption processing section generates a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the content (Scott: Figure 1 : the predefined table as taught by Scott is interpreted as a predetermined number of bytes on the content to meet the claim language).

Art Unit: 2131

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Scott within the system of Orrin because Scott teaches an alternative digital data content integrity validation mechanism by generating a hash value from a file key (Scott: Column 1 Line 5 – 8).

Accordingly, Orrin in view of Scott teaches when said contents block data contains a plurality of parts and it is one part that needs to be verified, said encryption processing section generates a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the entire decrypted statement obtained by decryption processing of parts (Orrin: Column 7 Line 40 – 41: a decrypted text from an encrypted content is equivalent to a plain text) to be verified in the case where said parts to be verified is encrypted, and generates a contents check value by executing encryption processing applying said contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on said entire part to be verified in the case where said parts to be verified is not encrypted (Orrin: Column 7 Line 13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67; Scott: Column 1 Line 5 – 8).

As per claim 17, 18, 34, 35, 103, 104, 105, 110, 116, 117, 118, 123, 129, 130 and 135, claim 17, 18, 34, 35, 103, 104, 105, 110, 116, 117, 118, 123, 129, 130 do not further teach over claims 109 as addressed above.

Art Unit: 2131

10. Claims 106, 119 and 131 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Scott (Patent Number: 5199073), in view of Teppler (Patent Number: 6898709).

As per claim 106, 119 and 131, Orrin as modified does not disclose expressly said encryption processing section has an encryption processing configuration in CBC mode and said decryption processing applied to the content intermediate value generation processing when the contents block data to be verified is decryption processing in CBC mode.

Teppler teaches said encryption processing section has an encryption processing configuration in CBC mode and said decryption processing applied to the content intermediate value generation processing when the contents block data to be verified is decryption processing in CBC mode (Teppler: Column 7 Line 12 – 24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Teppler within the system of Orrin because Teppler teaches providing the assurance of the integrity of digital data files with enhanced fraud prevention mechanisms (Teppler: Column 16 Line 36 – 52).

Art Unit: 2131

11. Claims 16 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Bodo (Patent Number: 5680587), and in view of Nessett (Patent Number: 6055236).

As per claim 16 and 33, Orrin teaches a digital signature stored in the header section (Orrin: Column 8 Line 1 – 3). However, Orrin does not disclose expressly collating only the header section integrity check values in the data during the process executed by said cryptography process section to collate the partial integrity check values.

Nessett teaches collating only the header section integrity check values in the data during the process executed by said cryptography process section to collate the partial integrity check values (Nessett: Column 23 Line 40 – 45).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Nessett within the system of Orrin because (a) Orrin discloses a basic key transfer process utilized by the file and document security systems via electronic mail or a network system through a horizontal trust model (Orrin: Column 4 Line 21 – 3) and (b) Nessett teaches providing enhanced internet security services using authentication header (Nessett: Column 3 Line 44 – 50).

According Orrin as modified teaches collating only the header section integrity check values in the data during the process executed by said cryptography process section to collate the partial integrity check values and transmitting data for which collation of the header section integrity check values



Art Unit: 2131

has been established, to said reproduction process section for reproduction (Orrin: Column 4 Line 21 – 3; Bodo: Column 13 Line 16 – 25 and Nessett: Column 3 Line 44 – 50).

12. Claims 107, 120 and 132 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (Patent Number: 6011849), in view of Scott (Patent Number: 5199073), in view of Teppler (Patent Number: 6898709), and in view of Kuroda (Patent Number: 6915434).

As per claim 107, 120 and 132, Orrin as modified does not teach using a common key encryption process (Kuroda: Abstract Line 1 – 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kuroda within the system of Orrin because Kuroda teaches providing a key management function in an electronic data storage system for guaranteeing the security of electronic data by changing the key used in a process of encrypting electronic data in document form in a local environment and a global environment (Kuroda: Column 1 Line 10 – 16).

Accordingly, Orrin as modified teaches the encryption processing configuration in CBC mode of said encryption processing section is a configuration in which common key encryption processing is applied a plurality of times only to part of a message string to be processed (Orrin: Column 7 Line

Art Unit: 2131

13 – 16, Column 7 Line 30 – 41 and Column 8 Line 54 – 67; Teppler: Column 7 Line 12 – 24 and Kuroda: Abstract Line 1 – 10).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
LBC

Longbit Chai  
Examiner  
Art Unit 2131

  
Primary Examiner  
AU2131  
9/23/05